FINANCIAL INSTITUTIONS TODAY

News and topics of interest to financial institutions regulated by the Department of Banking and Finance

July 2016

Inside this issue:

Guidance for Managing Ransomware Threats

The Treasury Department together with U.S. intelligence and regulatory agencies have jointly released an interagency technical guidance document on how institutions can better manage ransomware threats. The document provides an aggregate of already existing federal government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents. The guidance is available at http://csbs.informz.net/csbs/data/images/How%20to%20Protect%20Your%20Networks%20from%20Ransomware_%20Technical%20Guidance%20Documen.pdf.

Annual Assessment for State-Chartered Financial Institutions

The Department will email annual assessment fee letters to Georgia state chartered banks and credit unions in August, and the **fees will be assessed on September 15, 2016**.

Please complete and submit any change of information by August 31, 2016, using the Electronic Funds Transfer ("EFT") Authorization Form. The EFT Authorization Form and Instructions can be found on the Department's website at: http://dbf.georgia.gov/documents/electronic-funds-transfer-authorization-form-and-instructions.

Please contact Chris Pittman with any questions at cpittman@dbf.state.ga.us or 770-986-1641.

Annual Assessment for Bank Holding Companies

The Department will email the annual holding company assessment fee letters to supervised bank holding companies in August. **The fees are due by September 15, 2016, and online reporting/payment is mandatory** through the Department's website at: https://bkgfin.dbf.state.ga.us/HCAssessments.html.

Please contact Chris Pittman with any questions at cpittman@dbf.state.ga.us or 770-986-1641.

Wire Transfers

Using a financial institution to send funds electronically has become a fast, convenient, and frequently used tool for customers and members of financial institutions. Wire transfers have additional risk exposure because the transactions are both immediate and irrevocable. In addition, wire transfer fraud continues to rise and evolve. Social engineering plays an increasingly large role in wire transfer fraud, with perpetrators researching companies and financial institutions for weaknesses in controls that can be manipulated. Most vulnerable are the financial institutions and business customers that have not implemented and adhered to

robust solutions to mitigate risk. The Board of Directors (Board) of each financial institution should ensure that adequate policies are in place, and management should implement appropriate risk management practices.

The Board should also fully understand the limits of the fidelity bond coverage. Financial institutions are audited and examined to determine if security procedures satisfy prevailing standards. If an institution does not have adequate controls or does not adhere to them, fraudulent transactions that might otherwise be covered may be disallowed. For example, policies that do not include appropriate limits could be considered to be ineffective controls. The dollar amount authorized in the Board's policy may be "unlimited" or so large that it is effectively unlimited which results in no reasonable mitigation of the loss exposure amount. Also, authorization or other access to wire transfers may not be limited to personnel whose job responsibilities require access, resulting in the lack of appropriate risk mitigation practices. The Department encourages the Boards of financial institutions to review policies for internal controls addressing wire transfers. In addition, the Board should periodically assess the adequacy of insurance coverage to limit the financial exposure to wire transfer fraud. Moreover, the Board should read its policy closely to determine if coverage specifically excludes loss from certain funds transfer transactions such as a forgery exclusion. If such an exclusion is present, the Board may want to consider adding a rider to the policy.

Management should look closely at wire transfer operations, ensuring not only that adequate internal controls are developed, but also that controls are not being circumvented for convenience and a desire to make the transactions more user friendly for the customer or member. In the short run, these results may seem desirable, but neglect of the established controls can result in losses that may not be recoverable. Department examiners report instances in which the list of individuals authorized to execute wires includes individuals who no longer work for the financial institution, controls requiring two individuals to approve the transfer are circumvented when one of authorized individuals provides the information necessary to another individual without actually reviewing the transaction, confirmations are not performed, or contact information has been changed by someone not affiliated with the customer. Management should consider customer or member education as a valuable component of risk mitigation. The Board should take steps to implement an effective system to evaluate compliance with established internal controls that ensures continuous updates to policies, as appropriate.

One of the more frequent scams is known as a corporate account takeover (CATO), which involves the perpetrator posing as a company executive calling to request a wire transfer, frequently to a foreign financial entity, that needs to be executed quickly. The perpetrator is counting on weaknesses in controls that would lead to failure to confirm the wire transfer request. This scam was discussed in a previous *Financial Institutions Today* article, with links to guidance that discussed appropriate internal controls that would mitigate risk to financial institutions that are targeted for fraudulent wire transfers. http://dbf.georgia.gov/sites/dbf.georgia.gov/files/related_files/document/February2013Bulletin.pdf. A variation on CATO that recently emerged has been business email compromise (BEC). FS-ISAC and federal law enforcement agencies have released a joint alert warning companies of BEC which is available at https://www.fsisac.com/sites/default/files/news/BEC_Joint_Product_Final.pdf.

Vendor Management

Outsourced Information Technology Services

Financial institutions depend on third-party service providers to support critical operations and meet customer service needs. As such, Boards and management teams must maintain proper oversight and risk management of outsourced information technology functions. The Board is responsible for establishing an appropriate risk management program to manage relationships with technology service providers. This program should be focused on the primary goals of any information technology program: maintain confidentiality of sensitive data, ensure data is accessible at the time it is needed, and ensure integrity of data during storage and transmission. An effective vendor management program provides the opportunity for institutions to identify weaknesses in outsourcing relationships that may compromise confidentiality, accessibility, and integrity and take appropriate action before problems arise.

The Federal Financial Institutions Examinations Council (FFIEC) Information Technology Examination handbook "Outsourcing Technology Services" provides guidance to financial institutions for evaluating risk management processes to establish, manage, and monitor outsourcing relationships.

Typically, oversight of outsourcing relationships incorporates the following activities:

- Risk assessment and requirements definition;
- Due diligence in selecting a service provider;
- Contract negotiation and implementation; and
- Ongoing monitoring.

Key elements of an effective risk management program include:

- Establishing senior management and Board awareness of the risks associated with outsourcing agreements in order to ensure effective risk management practices;
- Ensuring that an outsourcing arrangement is prudent from a risk perspective and consistent with the business objectives of the institution;
- Systematically assessing needs while establishing risk-based requirements;
- Implementing effective controls to address identified risks;
- Performing ongoing monitoring to identify and evaluate changes in risk from the initial assessment; and
- Documenting procedures, roles/responsibilities, and reporting mechanisms.

In addition, institutions are partially or completely outsourcing information security functions to third-party service providers, known as Managed Security Service Providers (MSSP's). Examples of well-known MS's in the financial sector include Dell SecureWorks and ProfitStars Gladiator Tech. While institutions may gain needed expertise and cost benefits from relationships with MS's, proper management of these relationships require enhanced risk management controls. In addition to the normal management responsibilities, a successful engagement with an MSSP should include:

- A contract with mutually agreed upon Service Level Agreements (SLAs);
- Strategies for ensuring transparency and accountability that include:
  - Regular communication between the financial institution and the MSSP on matters including change control, problem resolution, threat assessments, and management information systems reporting,
  - Descriptions of processes for physical and logical controls over financial institution data; and
- Periodic review of the MSSP's processes, infrastructure, and control environment through offsite reviews of documentation and onsite visitations.

Institutions are also expected to incorporate relationships with outsourced service providers into Disaster Recovery and Business Continuity Plans. In February 2015, the FFIEC updated the “Business Continuity Planning” booklet by adding *Appendix J: Strengthening the Resilience of Outsourced Technology Services*. Most importantly, the appendix stresses the need for institutions to ensure that relationships with outsourced service providers will not negatively affect their ability to appropriately recover critical functions in a timely manner. This appendix discusses four key elements of business continuity planning that a financial institution should address to ensure they are contracting with services providers that are strengthening the resilience of technology services:

- Third-party management addresses a financial institution management's responsibility to control the business continuity risks associated with service providers and their subcontractors.
- Third-party capacity addresses the potential impact of a significant disruption on a servicer's ability to restore services to multiple clients.
- Testing with service providers addresses the importance of validating business continuity plans with technology service providers and considerations for a robust third-party testing program.
- Cyber resilience covers aspects of business continuity planning unique to disruptions caused by cyber events.

Outsourcing technology services can provide a significant benefit from a cost and expertise standpoint, but requires the necessary oversight to manage the related risks. Institutions should utilize the interagency information technology handbooks as guide for establishing a strong risk management framework and should regularly evaluate the quality of their risk management programs as both the institution and technologies continue to evolve.

Action on Applications for the Month:

The following is a summary of official action taken on applications by state financial institutions under Title 7, Chapter 1 of the O.C.G.A. and petitions for certificate of incorporation of financial institutions and other matters of interest during the month of July 2016.

FINANCIAL INSTITUTION CONVERSIONS

PREVIOUS NAME	CONVERTED TO	APPROVAL DATE	EFFECTIVE DATE
American Commerce Bank, National Association	American Commerce Bank Bremen Haralson County	Pending	

APPLICATIONS TO ESTABLISH A BRANCH OFFICE

FINANCIAL INSTITUTION	BRANCH OFFICE	APPROVAL DATE	BEGIN BUSINESS DATE
Georgia's Own Credit Union Atlanta	Roswell 1184 Alpharetta Street Alpharetta, GA 30075 Fulton County	07-27-2016	
SunTrust Bank Atlanta	Decatur Crossing 2591 Blackmon Drive Decatur, GA 30033 DeKalb County	07-15-2016	
SunTrust Bank Atlanta	Magothy Gateway 157 Ritchie Highway Severna Park, MD 21146 Anne Arundel County	07-15-2016	
The Southern Credit Union Fayetteville	Kia 7777 Kia Parkway West Point, GA 31833 Troup County	05-25-2016	07-11-2016
Ameris Bank Moultrie	Riverplace Tower 1301 Riverplace Boulevard Jacksonville, FL 32207 Duval County	02-12-2016	07-13-2016
Robins Financial Credit Union Warner Robins	Russell Parkway Land Lot 96, Russell Parkway Warner Robins, GA 31088 Houston County	07-01-2016	

APPLICATIONS TO CHANGE LOCATION

FINANCIAL INSTITUTION	CHANGE LOCATION OF	APPROVAL DATE	EFFECTIVE DATE
SunTrust Bank Atlanta	The Galvan From: 1701 Rockville Pike Rockville, MD 20852 Montgomery County To: 1800 Rockville Pike Rockville, MD 20852 Montgomery County	Pending	

Associated Credit Union Atlanta	Decatur From: 1 West Court Square Decatur, GA 30030 DeKalb County To: 2641 E. College Avenue Decatur, GA 30030 DeKalb County	07-22-2016

NOTICE OF CHANGE IN NAME

PREVIOUS NAME	NEW NAME	APPROVAL DATE	EFFECTIVE DATE
Ethicon Credit Union Cornelia	North Main Credit Union	07-19-2016	

APPLICATION FOR RESERVATION OF A NAME

PROPOSED NAME	COUNTY	APPLICANT
The Peoples Bank of Georgia	Talbot County	Mr. Henry M. Persons President/CEO The Peoples Bank of Talbotton P.O. Box 158 Talbotton, GA 31827-0158

FINANCIAL INSTITUTION MERGERS

FINANCIAL INSTITUTION (SURVIVOR)	MERGED INSTITUTION	APPROVAL DATE	EFFECTIVE DATE
First National Bank of Decatur County Bainbridge, GA	Citizens Bank Cairo, GA	Pending	
United Community Bank Blairsville, GA	Tidelands Bank Mount Pleasant, SC	06-24-2016	07-01-2016
Bank of the Ozarks Little Rock, AR	Community & Southern Bank Atlanta, GA	07-18-2016	07-20-2016
State Bank and Trust Company Macon, GA	The National Bank of Georgia Athens, GA	Pending	

APPLICATIONS TO BECOME A BANK HOLDING COMPANY AND/OR TO ACQUIRE VOTING STOCK OF A FINANCIAL INSTITUTION

BANK HOLDING COMPANY	TO ACQUIRE	APPROVAL DATE
Southeast, LLC Atlanta, GA	Barwick Banking Company Barwick, GA	Pending
Bainbridge Bancshares, Inc. Bainbridge, GA	Citizens Bank Cairo, GA	Pending
Peach State Bancshares, Inc. Gainesville, GA	Peach State Bank & Trust Gainesville, GA	07-06-2016

DBF OUTREACH

AND UPCOMING SPEAKER ENGAGEMENTS:

- 7th Annual CBA Georgia Bank Directors' College - Commissioner Kevin Hagler will be speaking at the 7th Annual CBA Georgia Bank Directors' College, presented by the Community Bankers Association of Georgia, at The Ritz-Carlton Lodge, Reynolds Plantation, Greensboro, Georgia, on August 22, 2016. For more information about this event, visit http://web.cbaofga.com/events/7th-Annual-CBA-Georgia-Bank-Directors%E2%80%99-College-82216-4184/details.

- De Novo Conference - Commissioner Hagler will be speaking at the De Novo Conference, presented by the Georgia Bankers Association, at the Cherokee Town and Country Club, Atlanta, Georgia, on September 14, 2016. Visit http://gbacareerpaths.gabankers.com/Lists/Calendar%20of%20Events/DispForm.aspx?ID=10874&Source=http%3A%2F%2Fgbacareerpaths.gabankers.com%2FLists%2FCalendar%2520of%2520Events%2FCalendar%2520View.aspx for more information about this event.

Sign-up to Receive this Publication:

This publication is delivered to interested parties via e-mail and is also available from the Department's website at: http://dbf.georgia.gov/ under Publications, **Financial Institutions Bulletin**.

If you would like to be added to our distribution list, send an e-mail to dbfpress@dbf.state.ga.us stating your name and e-mail address. Please be sure to include "**Subscribe to Financial Institutions Bulletin"** in the Subject line.

The Department is the state agency that regulates and examines Georgia state-chartered banks, state-chartered credit unions, state-chartered trust companies, and bank holding companies that own Georgia state-chartered financial institutions. The Department also has responsibility for the supervision, regulation, and examination of Merchant Acquirer Limited Purpose Banks (MALPBs) chartered in Georgia.

In addition, the Department has regulatory and/or licensing authority over mortgage brokers, lenders and processors, mortgage loan originators, check cashers, sellers-issuers of payment instruments, money transmitters, and international banking organizations.

Our **Mission** is to promote safe, sound, competitive financial services in Georgia through innovative, responsive regulation and supervision.

Our **Vision** is to be a willing and able partner with our regulated entities in order to support vibrant economic growth and prosperity in Georgia.

Department of Banking and Finance
2990 Brandywine Road
Suite 200
Atlanta, Georgia 30341-5565

Phone: (770) 986-1633
Fax: (770) 986-1654 or 1655
http://dbf.georgia.gov/
Email: dbfpress@dbf.state.ga.us